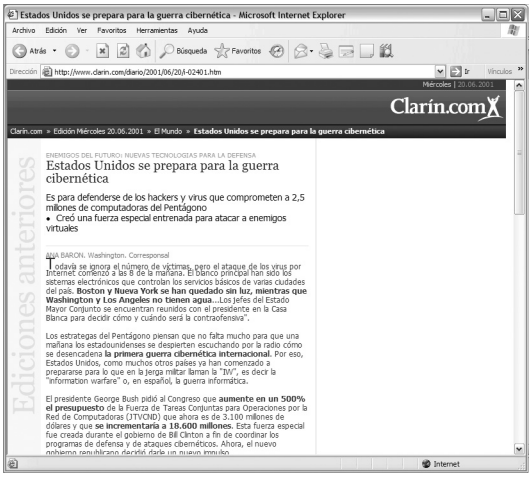
SXC BUZZYBEE

LAS ORGANIZACIONES MILITARES FRENTE A UN NUEVO ESCENARIO, LA GUERRA INFORMÁTICA

Augusto S. Rivolta

El Teniente de Navío Augusto Sebastián Rivolta egresó de la ESNM en diciembre de 1994, como Guardiamarina de Cuerpo Comando, Escalafón Naval (Promoción 124).
Se desempeñó en los siguientes destinos: LHPE (Jefe de cargo), cazaminas ARA Formosa *(Jefe Operaciones), aviso ARA* Alférez Sobral *(Jefe Armamento), lancha rápida ARA* Intrépida *(Jefe Armamento), corbeta ARA* Spiro *(Jefe de cargo), patrullero ARA* Murature *(Segundo Comandante), transporte ARA* Cabo de Hornos *(Segundo Comandante).*
En 1997 realizó el Curso Básico de Capacitación en Artillería (ESOA).
Durante el año 2004 realizó el Curso Superior de Defensa, en la Escuela Nacional de Defensa. En el 2006 realizó el Curso Aplicativo para Oficiales Navales (ESOA).

Hoy tanto los ordenadores como las redes de transmisión de datos (Internet, networks, lands, etc.) se han convertido en una herramienta de uso diario, haciendo viables tareas disímiles, ofreciendo grandes ventajas. Su utilización va, desde un simple almacenamiento de datos hasta el manejo de complejas instrucciones, por ejemplo operar mecanismos de autodefensa antimisil. Así mismo la necesidad de redes y los avances tecnológico-informáticos han permitido derribar la barrera de límites físicos, creando las condiciones para utilizar la informática como una herramienta bélica.


Estados Unidos se prepara para la guerra cibernética - Microsoft Internet Explorer

Clarín.com

Clarín.com » Edición Miércoles 20.06.2001 » El Mundo » Estados Unidos se prepara para la guerra cibernética

ENEMIGOS DEL FUTURO: NUEVAS TECNOLOGÍAS PARA LA DEFENSA

Estados Unidos se prepara para la guerra cibernética

Es para defenderse de los hackers y virus que comprometen a 2,5 millones de computadoras del Pentágono

- Creó una fuerza especial entrenada para atacar a enemigos virtuales

ANA BARON. Washington. Corresponsal

Todavía se ignora el número de víctimas, pero el ataque de los virus por Internet comenzó a las 8 de la mañana. El blanco principal han sido los sistemas electrónicos que controlan los servicios básicos de varias ciudades del país. **Boston y Nueva York se han quedado sin luz, mientras que Washington y Los Angeles no tienen agua**...Los Jefes del Estado Mayor Conjunto se encuentran reunidos con el presidente en la Casa Blanca para decidir cómo y cuándo será la contraofensiva".

Los estrategas del Pentágono piensan que no falta mucho para que una mañana los estadounidenses se despierten escuchando por la radio cómo se desencadena **la primera guerra cibernética internacional.** Por eso, Estados Unidos, como muchos otros países ya han comenzado a prepararse para lo que en la jerga militar llaman la "IW", es decir la "information warfare" o, en español, la guerra informática.

El presidente George Bush pidió al Congreso que **aumente en un 500% el presupuesto** de la Fuerza de Tareas Conjuntas para Operaciones por la Red de Computadoras (JTVCND) que ahora es de 3.100 millones de dólares y que **se incrementaria a 18.600 millones.** Esta fuerza especial fue creada durante el gobierno de Bill Clinton a fin de coordinar los programas de defensa y de ataques cibernéticos. Ahora, el nuevo

Ediciones anteriores

A raíz de esta situación se comienza a hablar a nivel mundial, de la "Guerra Informática". El objetivo es afectar de algún modo a un ordenador o a la red de interés (con los efectos que las trascienden) para entorpecer, dañar, modificar o destruir su capacidad operativa; lo cual es posible con el envío de instrucciones en su amplísimo alcance (virus, script, gusanos).

Enemigos del futuro:
Nuevas tecnologías para la defensa
Estados Unidos se prepara para la guerra cibernética
www.clarin.com/diario/2001/06/20/i-02401.htm

Algunos autores, como Winn Schwartau, experto norteamericano en seguridad informática, subdivide el escenario de la guerra informática en tres clases en función de los actores que intervienen *(1)*.

Clase 1: Guerra antipersonal: Esta subdivisión incluye los ataques contra la privacidad de los datos personales. Esto implica la revelación (o búsqueda no autorizada) de datos existentes en bases de datos que se suponen confidenciales, o su alteración.

(1)
www.seas.gwu.edu/student/reto/infowar/info-war.html

BOLETÍN DEL CENTRO NAVAL
Número 819
Enero / marzo de 2008
Recibido: 11.9.2007

Un ciudadano promedio tiene hoy muy poca posibilidad de controlar los datos que le conciernen y que han sido recopilados por diversas empresas (al abrir una cuenta corriente, al obtener y utilizar una tarjeta de crédito, al contestar encuestas, etc.), si embargo estos datos no sólo pueden ser obtenidos ilegalmente por operadores del oponente, sino que pueden ser vendidos y alterados por quienes los poseen. Los países de la Unión Europea formulan leyes bastante exigentes en torno a la protección de datos personales y están desalentando el comercio electrónico con países que no tienen leyes equivalentes.

La nueva amenaza en internet: los espías informáticos

Nota:

En el mundo de la seguridad informática el caso Kinko representa una seria amenaza a la privacidad de los usuarios de Internet y tanto los particulares como las empresas corren el riesgo de perder el control de su información más confidencial.

Este año Juju Jiang, un joven de 25 años que vive en Nueva York, admitió haber plantado el denominado 'keylogging software' en computadoras públicas de 13 puntos de ventas de fotocopiadoras Kinko en todo Manhattan. El software le permitió grabar y robar información personal a más de 450 personas. Usó esa información para transferir fondos de las cuentas bancarias de sus víctimas a cuentas nuevas que él mismo había abierto a su nombre. También vendió por Internet los datos que había robado.

Fuente: EmpresasNews

Ataque a Internet: 80.000 máquinas zombis en Corea

Por José Luis López

Las investigaciones de las autoridades de diferentes países, han seguido las pistas de quienes intentaron sabotear a los trece servidores raíz encargados de la traducción de nombres a partir de direcciones IP en Internet, ocurrido hace pocas semanas (ver "Ataque global a la red DNS"). Si bien estas computadoras son las más importantes de la red, los expertos piensan que este ataque no fue la forma más eficiente para afectar el funcionamiento de la misma. Aunque sí se trató del ataque coordinado más maligno y ambicioso en la historia de Internet.

Fuente: http://www.vsantivirus.com/03-11-02.htm

Clase 2: Guerra corporativa: Este es el tipo de guerra que pueden mantener corporaciones y empresas de todo el orbe, recurriendo a métodos de intrusión informática para penetrar los sistemas de sus oponentes, obtener acceso a sus bases de datos y a los resultados de sus investigaciones. Podrían incluso destruir antecedentes, haciendo que dicha destrucción parezca un accidente fortuito producto de un virus, poniéndose en ventaja en el desarrollo de nuevas tecnologías. Este tipo de acción no es nuevo y se conocen varios casos ocurridos durante la "Guerra Fría" en los EE.UU. y la URSS. Según un informe del Consejo de Estado de Francia, France Telecom sería objeto de 900 intentos de penetración de "hackers" por cada fin de semana. Sólo en 1995 el Departamento de Defensa Norteamericano detectó 38.000 ataques a sus sistemas [(2)].

(2) www.lemonde.fr/actu/nvtechno/cybercrime/speeches/dci_testimony_062498.html

Otra forma de combate es la difusión por Internet de información falsa. Durante la última guerra entre EE.UU. e Iraq, las cadenas de noticias CNN y Alyacira saturaron de información los medios de comunicación y la web, provocando desconcierto y desconfianza en la población mundial.

Estados Unidos prepara defensas ante una ciberguerra

15/nov/02

El Congreso estadounidense aprobó una partida de US$ 900 millones para impulsar programas orientados a luchar contra un potencial ataque terrorista contra los sistemas informáticos de ese país.

Fuente: Wired News.con

Otro ejemplo lo tuvimos en la Argentina cuando salió a conocimiento público la venta de un reactor nuclear, fabricado por el INVAP, a Australia, donde los sitios de Internet nacionales brindaban información de todo tipo en función de sus intereses, dividiendo la opinión pública. Llegando a poner en peligro la venta del reactor.

Clase 3: Guerra global: Esta categoría se aplica tanto a las relaciones entre industrias y poderes económicos como entre naciones. Ya no se trata de robar secretos o producir algún daño limitado sino de recurrir a métodos que permitan destruir al enemigo. Aquí los recursos a invertir son lo de menos porque, aunque cuantiosos, son menores que los que se requerirían para una guerra convencional. La CIA plantea que sus futuros enemigos no pretenderán atacar el país con armas nucleares sino penetrando en sus sistemas informáticos y causando verdadero daño a su poderío militar y a su economía. ¿Y por qué los terroristas van a elegir este tipo de acciones? Pues hay dos razones de peso. La primera es que a través de Internet se mueven billones de dólares en pequeñas transacciones comerciales con una protección bastante baja. La segunda razón es que se pueden causar desastres militares casi tan graves como los que se pueden ocasionar en el campo de batalla, y sin salir de casa *(3)*.

(3) www.cia.gov/cia/public_affairs/speeches/dci_testimony_062498.htm

Hackers controlan satélite militar británico
(02.03.99): Satélite militar de comunicaciones está siendo controlado por piratas informáticos. El satélite sería usado para la defensa de Gran Bretaña en caso de un ataque nuclear. Según el diario inglés, desconocidos alteraron el rumbo del satélite hace dos semanas, luego de lo cual las autoridades responsables recibieron una extorsión según la cual los hackers dejarían en paz el satélite a cambio de una fuerte suma de dinero en efectivo.
Fuente: Sunday Business

Dentro de este escenario virtual se convive con la práctica de todo tipo de operaciones, donde los operadores tienen el mismo grado de preeminencia y sus capacidades van de la mano de la creatividad y el conocimiento. Por ello la actividad de hacking, intrusión, penetración de sistemas, monitoreo de tráfico, scanneo de sistemas, finger printing, o cualquier indeseable fenómeno de este tipo, no debe ser pensada como realizada por un delincuente común, sino por un adversario inteligente. Cabe aclarar que la mayoría de las veces se encuentran financiados por diferentes actores, como estados, gobiernos, corporaciones, etc. Hoy cualquier agencia de inteligencia seria está en capacidad de explotar este recurso.

Hacker ataca sitio oficial de la Presidencia de la Nación Argentina
18/07/06
Nota:
El sitio oficial de la Presidencia de la Nación Argentina fue atacado, arrojando como consecuencia la alteración de los textos de uno de los discursos del Presidente Néstor Kirchner.
Fuente: www.presidencia.gov.ar

La seguridad informática en el ejército norteamericano es deficiente
11:00 - 22/03/2006
Una auditoría en los sistemas informáticos responsables de los radares, lanzamientos de mísiles y centros de mando tenía graves deficiencias en aspectos de seguridad.
Fuente: HISPASEC.COM

Ante un nuevo escenario

Como se pudo observar, el concepto de guerra informática se hace cada vez más común en las operaciones militares. De tomar conciencia que dentro de ella se desarrollarán tanto acciones ofensivas como defensivas, las Fuerzas Armadas deberán elaborar sus estrategias dentro de este escenario para direccionar sus futuras acciones. Esto obliga a reflexionar sobre la informática pensándola de manera distinta, no como una simple herramienta para agilizar tareas, sino como un nuevo ambiente de guerra. Donde la táctica, la técnica y la formulación de doctrina se combinan para cumplir con propósitos tácticos y estratégicos específicos.

La amenaza de la guerra informática requiere mayor atención en todos los frentes

Nota: (Entrevista con el senador Jon Kyl)

Ni la administración, ni el Congreso, ni el público en general dedican la debida y suficiente atención a la creciente amenaza de una guerra informática (o guerra I), dice el senador Jon Kyl. Nuestros adversarios potenciales perfeccionan su capacidad de atacar las infraestructuras esenciales que cada vez más corren a cargo de las comunicaciones, el transporte y los sistemas financieros de nuestro país, así como de su vital sistema de defensa, advierte el senador. Kyl, republicano por Arizona, dirige la Subcomisión de Tecnología, Terrorismo y Estado de la Comisión de lo Judicial del Senado. Es también miembro de la Comisión del Senado sobre Asuntos de Inteligencia. Kyl fue entrevistado por el redactor colaborador Ralph Dannheisser.

Fuente: Publicación Electrónica del USIS, Vol. 3, No. 4, noviembre de 1998

No es difícil de imaginar las grandes ventajas que puede obtener el enemigo, si consigue penetrar en los sistemas informáticos de su oponente en tiempos de paz o guerra. Sobre todo a mínimos costos y, lo más importante, bajo el anonimato.

En el plano regional, se puede afirmar que las fuerzas armadas no cuentan con un grado de dependencia tecnológico informático tal, que un ataque de esta naturaleza pudiera poner en peligro la ejecución de una operación; como sí puede ocurrir con las principales potencias mundiales, donde la utilización de satélites, Forcenet *(4)* u otros sistemas, los obligan a tomar activa participación en este teatro. Pero no se puede ignorar que las Fuerzas Armadas regionales se apoyan fuertemente en sistemas digitales para el manejo y resguardo de la información. Como se viene exponiendo, inexorablemente se expone ante las vulnerabilidades de la tecnología informática, obligándonos por lo menos a pesar en ello.

(4)
Es la Intranet que provee la arquitectura necesaria para incrementar sustancialmente las capacidades de combate mediante sistemas, funciones y misiones integradas. Transformará el conocimiento de la situación, acelera la velocidad para la toma de decisiones y permite una mejor y mayor distribución del poder de combate. Utiliza la información disponible para las operaciones de combate basadas en el conocimiento e incrementa la capacidad de supervivencia de la fuerza.

Otro fenómeno es el del personal que posee computadoras propias y tiene almacenada en ella información de los trabajos cotidianos que realiza y que además tiene su conexión a Internet. Este tipo de blanco resultará ser más rentable, por la facilidad de intrusión y obtención de la información, ya que estarán en una condición más desfavorable que las redes de las fuerzas; y si se sabe dónde buscar puede que se consiga información mucho más valiosa. Esto implicaría una fuga inocente de información de gran importancia, producto de la falta de concientización. Presentándose de esta manera, otro frente para que ataque un oponente.

Un hecho significativo a tener en cuenta es que con sólo una computadora integrante de una red que tenga acceso a Internet quedará indefenso todo el sistema *(5)*.

(5)
Estadísticas dadas por el CERT afirman que el 91% de los ordenadores con conexión a Internet están infectados con algún tipo de virus o agente pasivo que podría desarrollarse cuando así se le ordene.

La complejidad existente en organizaciones con la magnitud de una fuerza militar pone en juego muchas variables a considerar para hacer frente a este tipo de amenazas, pero todas ellas convergen en el grado de acompañamiento que tenga el personal sobre dicha problemática.

Se pueden adquirir o elaborar, con el asesoramiento de personal competente, sistemas software más apropiados para la neutralización de los efectos de los ataques informáticos, aunque la sola adquisición de uno o varios productos sobre los cuales gravitar la seguridad informática no alcanza. Por ello, la fortaleza e integridad del sistema deberá radicar en la concientización y responsabilidad que tenga el personal integrante de la fuerza.

A continuación se proponen tres tópicos sobre los cuales se debería trabajar para la conformación de las medidas a corto y mediano plazo, necesarias para enfrentar este escenario.

Planificación de una política de seguridad informática que responda a las infraestructuras de las Fuerzas. Su formulación direccionará y regulará los alcances que se le quiera dar a esta problemática y permitirá la elaboración de doctrina propia para la defensa de nuestros sistemas.

Utilización de un sistema criptográfico de diseño propio. Es el único medio que permitirá cubrir el porcentaje de información "inocentemente fugada" del ámbito. Cuando se habla de

un sistema criptográfico se debe pensar no sólo en el diseño de claves con su responsable y consciente manejo, sino también en la elaboración de los algoritmos propios que le den fortaleza y resguardo al sistema.

Concientización del personal. Es el más importante de los tópicos enunciados. Es el pilar sobre el que se debe fundar nuestra defensa informática. Con el personal concientizado, y comprometido con los sistemas, las posibilidades de vulneraciones se acotarían considerablemente.

Pero para poder hacer viable este accionar se debería comenzar con medidas estructurales, que permitan crear el campo propicio para el desarrollo de dicha concientización en todos los niveles. Esto se logrará a través de la incorporación del concepto de guerra informática dentro de la doctrina. Ya que permitirá desarrollar las acciones necesarias para formar a todo el personal en el compromiso institucional de esta problemática, implementando el conocimiento y la aplicación de medidas de orden práctico que contribuyan, partiendo de un nivel individual hasta el institucional, a la protección de toda información. Posteriormente se podrán adoptar medidas activas, como el monitoreo de redes en busca de vulnerabilidades, fallas y aplicaciones de sistemas de detección de intrusiones, que permitan anticipar al oponente y evaluar los resultados de las acciones que se realicen.

Proa a la visión estratégica

La guerra informática es considerada por distintos analistas internacionales como uno de los teatros emergentes en el que es más probable que ocurra un futuro conflicto de nación a nación en el nivel estratégico. Además afirman que la misma cambiará la forma de conducir los combates a nivel de teatro operacional, y aún muchas de las actividades militares *(6)*.

(6)
Winn Schwartau, experto norteamericano en seguridad informática www.signaltonoise.net/library/hackenc.htm. De fecha 24/05/06.

Además sabemos que cuanto mayor es la dependencia tecnológica, mayor es la dependencia informática, por lo tanto mayores son las vulnerabilidades expuestas al oponente. Premisas que nos llevarían a sostener que para la Armada, enfocar el problema casi exclusivamente al resguardo de la información, representa un error sobre la apreciación del poder implícito de estas técnicas. Es así que debe orientar los esfuerzos para abarcar los procedimientos y métodos que le permitan volcar este potencial sobre las fuerzas del oponente, tanto en tiempo de paz como de guerra.

Se debe asumir que hoy la contienda informática es el modo de hacer la guerra en el dominio de la información, del mismo modo que la guerra naval se refiere al dominio del mar. Como se ha podido apreciar, a través de la guerra informática se puede incrementar enormemente el volumen de información, permitiendo mayor poder de análisis que redundará en la elaboración de apreciaciones que ampliarán el campo informativo de todas las órbitas de interés.

La incorporación de nuevas tecnologías origina transformaciones a realizar tanto físicas como psicológicas para dar cabida a nuevos paradigmas. Ésta es una de las tareas más difíciles de lograr, si no se tiene una visión estratégica que apuntale dicha transformación. La tecnología no es sólo un multiplicador de fuerzas, sino que a lo largo de la historia ha producido revoluciones en los asuntos militares generando nuevas formas de hacer la guerra. Esto siempre fue así cuando la interacción de la visión estratégica con las nuevas tecnologías fue concretada. Éste es el desafío de la guerra informática al que nos debemos enfrentar, si se logra entender el nuevo escenario que se está gestando.

Conclusión

A lo largo del presente artículo se pone en evidencia la existencia de un nuevo escenario bélico. En él, las instituciones militares regionales tienen competencia directa ya que poseen

información valiosa a resguardar. Las mismas deberán entender, aceptar y explotar este escenario, dada la real existencia de un oponente del que protegerse.

Así se sostiene que las Fuerzas Armadas, entre ellas nuestra Institución, deben tener claro que la tecnología informática va a ser el factor orientador de la futura forma de conflictos. Esto obligará la formulación de una visión estratégica, que fijará los criterios orientadores para seleccionar objetivos en la planificación militar y determinará las operaciones más convenientes, así como los requerimientos generales de organización.

Los cambios de paradigmas obligan a actualizar los modelos existentes, por ello la incorporación del concepto de guerra informática dentro de la doctrina naval permitirá incorporar la problemática en los distintos estratos de la Institución, creando el escenario adecuado para poder trabajar en las diferentes bases mencionadas anteriormente, haciendo factible su implementación. Esto permitirá generar el campo propicio para la gestación de la Visión Estratégica, que identificará los cambios de mayor prioridad y direccionará nuestra maniobra dentro de este nuevo ambiente hostil.

"LA INCORPORACIÓN DEL CONCEPTO "GUERRA INFORMÁTICA" EN LA DOCTRINA, PERMITIRÁ ELEVAR LA CONCIENCIA COLECTIVA, INDUCIENDO A QUE SE TOMEN LOS RECAUDOS NECESARIOS PARA EVITAR LAS FILTRACIONES Y RESGUARDARNOS BAJO UN MANTO INFORMÁTICO INEXPUGNABLE."

ALEA JACTA EST *(7)*

(7)
"La suerte esta echada" o, "Que vuelen los dados bien alto" pareado de Menandro, poeta y dramaturgo de la Nueva Comedia, pronunciada por Julio César al cruzar el río Rubicón.

BIBLIOGRAFÍA

- *www.govannom.org/modules.php?name=Seguridad&d_op=getit&lid=21*
- *www.es.wikipedia.org/wiki/DARPA (arpanet es.wikipedia.org/wiki/ARPANET).*
- *http://www2.ing.puc.cl/~dcolle/publica-ciones/guerra/biblio.htm. De fecha 20/05/06.*
- *www.seas.gwu.edu/student/reto/infowar/info-war.html*
- *Guerra Cibernética, Military Review I septiembre-octubre 2003.*
- *http://www.gtri.gatech.edu/res-news/rchnews.html de fecha 02/06/06.*
- *http://www.danworld.com/nettools.html de fecha 02/06/06.*
- *http://www.rediris.es/rediris/boletin/57/enfoque2. de fecha 06/08/08.*
- *http://www.cert.org-/advisories/CA-99-17-denial-of-service-tools.html*
- *Forcenet: Aplicación de la Intranet, un ejemplo práctico. Por Edwin L. Armistead, CCUSN.*
- *http://www.trytel.com/hack - de fecha 02/06/06.*
- *http://www.simtel.net/simtel.net- de fecha 18/08/06.*
- *http://www.fcw.com/article92665-03-20-06-Print*
- *http://www.fcw.com/article92668-03-20-06-Web*
- *http://www.airpower.maxwell.af.mil/apjinternational/apjs/1996/2trimes96/stein.html#stein#stein. La Guerra de Información por Doctor Gairpwereleorge J. Stein.*
- *http://www.quands.cat/2006/03/21.html#a6907*
- *Revista de publicaciones navales Tomo CXXXIV N°689. En julio del 2003.*
- *Revista de publicaciones navales Tomo CXXXIV N°691. 3er trimestre del 2005.*
- *Seguridad en Internet. Por Enrique Mario Saura, CF.*
- *Garfinkel, Simson L.: The Manchurian Printer, (C) 1995 (reseña en The Boston Sunday Globe, march 5, 1995, Focus Section, P. 83).*
- *www.cia.gov/cia/public_affairs/*
- *www.cia.gov/cia/public_affairs/speeches/dci_testimony_062498.html*
- *www.lemonde.fr/actu/nvtechno/cybercrime/speeches/dci_testimony_062498.html*
- *www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm*
- *www.tinet.org/~jcgg/H_Historicos/Radio_Nacional_de_Espana_en_Tetuan.htm*
- *http://www.elmundo.es/navegante/index.html*